EXHIBIT C

Bill.com, LLC, Plaintiff, v. Danielle Cox, Defendant.	**DECLARATION OF ROBERT BLENKINSOP IN SUPPORT OF PLAINTIFF'S EMERGENCY MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION AND SUPPORTING MEMORANDUM** Case No. 2:23-cv-00026

I, Robert Blenkinsop, pursuant to 28 U.S.C. § 1746, declare:

1. I am over the age of 18 and have personal knowledge of the matters contained herein. I could and would testify competently to such facts if called as a witness.

2. I am currently employed as a Staff Security Engineer in Bill.com, LLC's ("BILL") Security Operations Center. In my role at BILL, I am responsible for monitoring the security of BILL's electronic systems and networks, and investigating any alleged misuse of or improper access to those networks. I worked with Danielle Cox while she was employed by BILL and am familiar with her access to BILL's systems.

3. As a leader in BILL's Information Technology ("IT") group, Ms. Cox was afforded a higher level of administrative access to BILL's electronic networks in order to fulfill her duties. Specifically, in order to effectively accomplish her duties as one of the leaders of BILL's IT group, Cox was given "super administrator" credentials that allowed her to access virtually all of BILL's systems and information, including the email accounts of other employees as well as BILL's corporate Slack database.

4. While BILL's information is primarily generated from its headquarters in California, that information is available to its employees across the nation.

5. BILL has an Acceptable Use Policy governing its employees' use of electronic equipment and network. In fact, Ms. Cox was tasked with implementing that Acceptable Use Policy as a member of IT leadership. Among other things, the Acceptable Use Policy mandates that any confidential information stored on BILL's electronic and computing devices is the sole property of BILL, that employees like Ms. Cox have an obligation to report any unauthorized use of such information, that employees like Ms. Cox are only permitted to access such information to the extent it was authorized and necessary to fulfill their assigned job duties, and that employees like Ms. Cox are strictly prohibited from syncing personal iCloud or other cloud-based accounts to company-issued devices. A true and correct copy of that policy is attached hereto as Exhibit 1.

6. The Acceptable Use Policy further prohibits employees from using other employee's accounts, from taking any actions to "disable, damage or otherwise interfere with any security related features," or from attempting to gain unauthorized access to BILL's accounts.

7. BILL uses specialized software called Code42 Incydr to monitor and safeguard its electronic systems. The Code42 Incydr platform monitors employees' use of BILL's electronic equipment and networks, and provides alerts to members of the Security Operations Center in the event that suspicious activity is detected. Among other things, the Code42 Incydr platform alerts Security Operations Center staff if it appears that an employee is attempting to exfiltrate BILL's information through electronic means.

8. On December 19 , 2022, myself and other members of the Security Operations Center began an investigation into suspicious activity from Ms. Cox's BILL account. Upon

reviewing those alerts, we discovered that in the prior few weeks, Ms. Cox had accessed and downloaded significant amounts of company data using a Google Vault platform.

9. Google Vault is a retention and eDiscovery tool for Google Workspace that helps manage information governance, and allows BILL to export Google Workspace data such as Gmail messages, Drive files, and other data. Special Google Administrator accounts are required to access Google Vault. Based on her leadership role within BILL's IT organization, Ms. Cox had administrator-level access for Google Vault, Slack, and the other systems she accessed as detailed below.

10. Upon further investigation of the history of her access to BILL's systems, members of the Security Operations Center and I were able to determine that on December 2, 2022, Ms. Cox used her administrator credentials to access and download nearly 5,800 emails from the account of her supervisor, Steven Januario. The earliest email downloaded from Mr. Januario's account appears to have been sent on or about July 5, 2022, and the most recent email was sent on December 2, 2022.

11. Our forensic investigation, using electronic metadata provided by the Code42 Incydr tool, also determined that Ms. Cox used her company-issued laptop to download those emails. Once downloaded to Ms. Cox's company-issued laptop, the emails were then moved to a folder that is synced with an iCloud account with the name "danielle.cox@getdivvy.com". In my role, I am aware that BILL does not authorize the use of iCloud accounts by its employees.

12. The investigation that I conducted with other members of the Security Operations Center also looked into Ms. Cox's access to BILL's corporate Slack account. Slack is third-party

internal messaging software used by businesses, including BILL, to allow employees to electronically communicate throughout the workday.

13. Using audit logs provided generated by Slack, I was able to confirm that between November 30, 2022 and December 7, 2022, and again using her enhanced administrative credentials, Ms. Cox requested five different exports of data from BILL's corporate Slack account, including at least one manual export of the company's entire Slack database, *i.e*. the internal messaging of every employee of the company. In particular, on December 1, 2022, Ms. Cox exported the entire BILL Slack database for nearly a 4-month period: from July 4, 2022 through November 5, 2022. While the Slack audit logs indicate that these exports were done using Ms. Cox's credentials, there is no record of the exported information being transmitted to Ms. Cox's company-issued computer. Put differently, our forensics investigation indicates that Ms. Cox may have used a non-company computer to export that Slack information.

14. The forensic investigation that I conducted also indicated that between December 5, 2022 and December 20, 2022, Ms. Cox continued to use her BILL credentials in order to conduct searches through the email account of Mr. Januario, along with the accounts of two other individuals employed in BILL's People department.

15. My understanding is that Ms. Cox began a requested leave from BILL on December 5, 2022. Because BILL expected Cox to return from leave, it did not turn off her access to the company's systems or require the return of her company-issued computer on December 5, 2022. However, upon being alerted to Ms. Cox's conduct as described above on December 21, 2022, members of the Security Operations Center took steps to immediately suspend all of Ms. Cox's access to BILL's accounts and networks.

16. Upon learning that Ms. Cox had not yet returned her company-issued laptop, we also sent a remote command to that device to lock it, such that it would be difficult for anyone to access the data upon it. We are unable to confirm whether or not that command was successful: if Ms. Cox had simply disabled her internet connection, for example, the command would not have reached her device. Even if the command were successfully transmitted, someone with Ms. Cox's level of technical acumen may still be able to access the files stored on that device's hard drive.

17. As our investigation of Ms. Cox's activities continues, we continue to learn of more suspicious behavior while she was an employee of BILL. Just this week, I discovered an alarming incident that took place in December regarding BILL's email retention policy.

18. BILL's normal email retention policy is such that even "deleted" emails are permanently retained on BILL's servers. Our investigation revealed that on December 2, 2022, Ms. Cox changed the email retention settings on her account so that "deleted" emails would *not* be retained, but would instead be permanently deleted and rendered unrecoverable after just one day. Because BILL's systems only allow for such a change to be made to an entire group within the company, rather than a single user, Ms. Cox made that change to the retention policy not just for her own email account, but for the email accounts of nine other employees in the IT organization as well.

19. Even more concerning is the fact that Ms. Cox changed that email retention setting *back* to its original setting the following Monday morning, December 5, 2022. Put differently, Ms. Cox changed BILL's email retention policy on Friday (her last day before her leave began) to ensure that any emails she deleted from her account that day would be permanently deleted within 24 hours. Ms. Cox then waited until the following Monday, by which point any deleted emails

would be permanently gone and unrecoverable, in order to restore the retention settings to their previous state.

20. I cannot think of a single legitimate reason why Ms. Cox would change the email settings in this fashion only to restore them 72 hours later. While BILL was ultimately able to recover those emails, it appears that Ms. Cox was attempting to hide her unauthorized access to, and exfiltration of, BILL's data and systems on that Friday.

21. Ms. Cox's company-issued computer is a MacBook Pro laptop with the serial number c02zvae7md6m. My understanding is that, as of the date of this declaration, that device has not been returned to BILL despite repeated demands for its return.

[signature page follows]

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 11th day of January, 2023.

DocuSigned by:
Robert Blenkinsop
E1BB4AE462FD4D5...

Robert Blenkinsop

EXHIBIT 1

Acceptable Use Policy

Identifier	P.IT.001
Effective Date	March 1, 2022
Applicable to	All employees, contractors, external parties with access to the Bill.com network
Policy Owner	VP, Information Technology
Review Cycle	Annual

1. Acceptable Use Overview

Acceptable use defines how individuals must handle organizational resources including actions that are allowed and not allowed.

2. Purpose

The intent of the Acceptable Use Policy is to communicate expectations for Bill.com employees and contractors regarding access to and use of Bill.com information assets which include but not limited to information, electronic and computing devices, and network resources to conduct Bill.com business or interact with internal networks and business systems, whether owned or leased by Bill.com, the employee, or a third party. These rules are in place to protect users and Bill.com. Inappropriate use exposes Bill.com to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

The Bill.com Acceptable Use Policy applies to all employees, contractors, third parties, and any other individual or entity for which we employ, conduct business with and/or obtain services that require access to our network or sharing of data.

This policy is to be enforced in all jurisdictions where Bill.com and its subsidiaries operate in accordance with local or regional laws and regulations.

4. Policy

4.1 General Use and Ownership

- Bill.com confidential information stored on electronic and computing devices whether owned or leased by Bill.com, the employee or a third party, remains the sole property of Bill.com
- Users shall bear the responsibility for knowing and complying with applicable state and federal laws, rules and regulations, and contractual obligations when accessing Bill.com information assets
- Bill.com provides information assets as a resource to all employees, contractors, consultants, temporary and other workers. Each individual shall be responsible for properly using and protecting those resources
- Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of Bill.com proprietary information
- Users may access, use or share Bill.com proprietary information only to the extent it is authorized and necessary to fulfill their assigned job duties
- Use of external information systems to access the Bill.com system is prohibited unless the appropriate security controls are verified and deemed adequate with an approved connection or processing agreement by InfoSec and Legal
- Users' access to Bill.com information assets (e.g., customer data) shall be restricted to need-to-know and minimum necessary
- Users shall be responsible for the use and protection of Bill.com information resources by using effective access controls (e.g., passwords) and by safeguarding those access controls (e.g. disclosing passwords)
- Users are required to handle, label, and store confidential data in accordance with the Data and Information Classification Policy
- Connection to the Internet, or use of a website, is a privilege and not a right. Any abuse of that privilege can result in legal and/or administrative action
- Users shall be allowed to use Bill.com information assets:
    - To which they have been granted authorized access
    - For Bill.com business and research purposes
    - For incidental personal use (Employees are responsible for exercising good judgment regarding the reasonableness of personal use.)
- Users shall be allowed incidental personal use so long as those activities are legal and do not violate:
    - Bill.com policies, including our Code of Conduct and Ethics
    - Contractual obligations
    - The safety, security, privacy, reputational and intellectual property rights of others.
    - Applicable restrictions on political or commercial activities
- Users are prohibited from syncing their personal iCloud and/or gmail/g-drive accounts on their corporate-issued devices
- The IT team provides appropriate hardware and software to employees for Bill.com business use only

- Bill.com reserves the right to audit and monitor networks and systems activities on a periodic basis to ensure compliance with this policy. In the event that use is determined to be contrary to Bill.com policy or applicable law, appropriate measures shall be taken
- Users shall ensure that unattended equipment has appropriate protection
- Users shall log-off computing devices when the session is finished (i.e., not just switch off the PC screen or terminal)
- Users shall safeguard unattended information system output devices (e.g., printers) to prevent unauthorized individuals from obtaining the output

*Note: *Unless otherwise approved, employees and contractors with access to sensitive production data (i.e. bank partner data) seeking to temporarily work outside of U.S. or other approved jurisdiction or country of employment will have all such access disabled until return to primary location to ensure data is not processed outside of authorized boundaries*

4.2 Acceptable Password Use

- Passwords must be kept confidential and must not be written down or recorded electronically
- Passwords and accounts must not be shared. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited
- Personal and Bill.com (business) passwords must be different
- Temporary passwords shall be changed at the first log-on.
- Passwords must meet the minimum requirements of Bill.com's Password Policy
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 5 minutes or less

4.3 User Acknowledgement and Agreement

User will not engage in the following activities:

- Disclose or share any Bill.com confidential data to unauthorized parties without proper authorization or approval
- Post, use or transmit content that they do not have the right to post or use, for example, under intellectual property, confidentiality, privacy or other applicable laws
- Post, use or transmit unsolicited or unauthorized content, including, but not limited to, advertising or promotional materials, "Junk mail", "Spam", "Chain letters", "Pyramid schemes", political campaign promotional material, and any other form of unsolicited or unwelcome solicitation or advertising
- Infringe upon copyrighted material of any kind, including the unauthorized downloading, copying, displaying, and/or distributing of copyrighted material. All such works should be considered protected by copyright law unless specifically stated otherwise. Any use of Bill.com information assets (e.g. network, email system, website, etc.) to access, display, send, transfer, modify, store or distribute copyrighted material (e.g., video/movies, music/audio, images, documents, software, text, etc.) is strictly prohibited
- Post, use or transmit content that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer

software or hardware or telecommunications equipment or otherwise interfere with or disrupt Bill.com information assets
- Post or transmit content that is harmful, offensive, obscene, abusive, invasive of privacy, defamatory, hateful or otherwise discriminatory, false and misleading, incites an illegal act, or is otherwise in breach of one's obligations to any person or contrary to any applicable laws and regulations
- Intimidate or harass another
- Use or attempt to use another employee, contractor, consultant, temporary, and other workers' account, service, or personal information
- Remove, circumvent, disable, damage or otherwise interfere with any security related features
- Attempt to gain unauthorized access to Bill.com information assets, other user's accounts, computing devices or networks connected to Bill.com information technology resources, through hacking, password mining or any other means, or interfere or attempt to interfere with the proper working of Bill.com information assets or any activities conducted through those information assets
- Impersonate another person or entity, or falsely state or otherwise misrepresent one's affiliation with a person or entity
- Conduct any activities with the intention of creating and/or distributing malicious programs using Bill.com's network (e.g., viruses, worms, Trojan Horses, etc.)
- Install or use unauthorized or malicious software, or obtain data and software from external networks
- Fail to exercise appropriate caution when opening emails, attachments or accessing external web sites

All users shall read and acknowledge the Acceptable Use Policy before receiving access to information assets, be responsible for appropriately securing their computers and other electronic devices from misuse or theft by others; and for avoiding any use that interferes with others' legitimate access to and use of Bill.com information assets.

4.4 Monitoring

- While Bill.com desires to maintain privacy and to avoid the unnecessary interruption of activities, Bill.com reserves the right to investigate unauthorized or improper use of computing devices, which may include the inspection of personal data stored or transmitted on Bill.com's network. In the event that use is determined to be contrary to Bill.com policy or applicable law, appropriate measures shall be taken
- Information asset owners shall approve the use of information assets and take appropriate action when unauthorized activity occurs

5. Roles and Responsibilities

Role	Responsibilities
IT Team	Enforce the IT policy

Infosec	Support the development and enforcement of policies and standards

6. Policy Governance

This policy is owned by the individual designated as the VP, Information Technology of Bill.com.

Review of this policy is required at a minimum annually in line with the last review date indicated in the Revision History section of this document or at the time of significant changes to the internal or external environment.

All new employees and contractors must complete mandatory security awareness training inclusive of review of this policy and supporting security policies.

Policy exceptions must be submitted via request to InfoSec Governance Risk and Compliance (GRC) for review and decisioning. If approved, an exception is effective for one year from the approved date and must be renewed. If a request is rejected, the control owner must identify and document a plan of action to reach compliance with this policy.

7. Policy Compliance

Adherence to this policy will be verified through various methods, including but not limited to, periodic walk-throughs, internal and external audits, metrics, and feedback to the policy owner.

8. Policy Violations

Any known violations of this policy should be reported to the InfoSec GRC team at grc@hq.bill.com. Any Bill.com user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment.

9. Related Policies, Standards, and Procedures

Policy, Standard, and Procedure	**Purpose**
Written Information Security Program (WISP)	Provides definitive information on the prescribed measures used to establish and enforce the information security program at Bill.com.
Information Security Policy	Provides the directives that will ensure the highest degree of safeguarding of the data we collect, process, transmit and store.
Data and Information Classification Policy	To ensure that information is classified and

	protected in accordance with its importance to the organization.
Data and Information Handling Standard	Defines handling procedures for information in the various classification categories.
End User Device Standard	Establishes provisions for using, configuring, acquiring, accessing, maintaining, protecting, and securing end-user computing devices.

10. References

10.1 Bill.com Resources

Bill.com Policies and Procedures Wiki

10.2 Laws, Rules, Regulations & Other Requirements

- Sarbanes Oxley (SoX)
- New York Department of Financial Services (NYDFS)
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection regulation (GDPR)
- California Consumer Protection Act (CCPA)
- Payment Card Industry - Data Security Standard (PCI - DSS)
- FTC Safeguards

10.3 Best Practices

- National Institute of Standards and Technology (NIST)
- International Standards Organization (ISO) 27001 and 27002
- Secure Controls Framework (SCF)

10.4 Control References

Key Control Mapping: **NIST CSF**: PR.PT-2; **SCF**: CFG-04, HRS-05, HRS-05.1, HRS-05.5, NET-12.2; **ISO 27001**: A.8.1.3

11. Point of Contact

For questions on this policy or to escalate potential violations, please contact the InfoSec Governance Risk and Compliance (GRC) team at grc@hq.bill.com.

12. Terms and Definitions

None

Revision History

Version	Date	Author	Revisions	Approved By
2.0	2/19/2022	IT Team	Annual Review	Jonathan Chan
2.0	3/10/2022	Infosec GRC	Annual Review	Netsai Massetti
2.0	10/24/2022	Infosec GRC	Update made to section 4.1	Netsai Massetti